Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

DreamBus Botnet Exploiting A Critical Vulnerability in Apache RocketMQ

Date of Publication	Admiralty Code	TA Number
September 7, 2023	A1	TA2023357

Summary

First Seen: May, 2023
Malware: DreamBus
Impact: A critical vulnerability (CVE-2023-33246) in Apache RocketMQ servers enables remote code execution, leading to a surge in attacks, including the deployment of the DreamBus malware. Timely system updates are crucial to defend against these threats.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-33246	Apache RocketMQ Command Execution Vulnerability	Apache RocketMQ	✗	✓	✓
CVE-2023-37582	Apache RocketMQ Remote Code Execution Vulnerability	Apache RocketMQ	✗	✗	✓

Vulnerability Details

#1

A critical vulnerability (CVE-2023-33246) in RocketMQ servers was exposed in May 2023, allowing for remote code execution. Exploitation of this vulnerability was observed since June 2023. This led to a series of attacks where threat actors infiltrated systems and installed the DreamBus malware. The attacks started in early June, peaked in mid-June, and targeted multiple ports in addition to the default RocketMQ port.

#2

Initially, attackers used the "interactsh" tool for reconnaissance, assessing server vulnerabilities without causing damage. Starting on June 19th, they began downloading and executing a malicious bash script called "reketed" via TOR proxies or specific IP addresses. The "reketed" script's primary function was to download the DreamBus main module from a TOR hidden service and execute it.

#3 The DreamBus main module was an ELF Linux binary, also undetected by antivirus software. It executed base64 encoded strings, which were script files for various functions, including downloading other malicious modules.

#4 DreamBus had capabilities like pinging the server, executing commands, mining Monero cryptocurrency, and spreading via IT automation tools and SSH. To ensure persistence, DreamBus established services and cron jobs. Its main goal was to install a Monero miner, but its modular nature allowed for versatile malicious activities.

#5 Although CVE-2023-33246 was fixed in version 5.1.1 and 4.9.6, these fixed version still contains RCE in NameServer component, CVE-2023-37582, in update configuration function of the NameServer component.

#6 This vulnerability exists within the update configuration function of the NS component and can be exploited when NameServer lacks proper permission verification and NS addresses are inadvertently exposed on the extranet.

#7 To mitigate this risk, it is strongly recommended for users to upgrade their NameServer version to 5.1.2 or above for RocketMQ 5.x or 4.9.7 or above for RocketMQ 4.x to prevent these attacks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-33246	Apache RocketMQ: 4.2.0 - 5.1.0	cpe:2.3:a:apache:rocketmq:*:*:*:*:*:*:*:*	CWE-94
CVE-2023-37582	Apache RocketMQ: 4.2.0 - 5.1.1	cpe:2.3:a:apache:rocketmq:*:*:*:*:*:*:*:*	CWE-94

Recommendations

Apply Patch and Updates: Promptly apply security patches and updates to all software, especially for systems running RocketMQ. Ensure that you are using versions 5.1.2 or above for RocketMQ 5.x or 4.9.7 or above for RocketMQ 4.x to mitigate these vulnerabilities.

Network Segmentation: Implement network segmentation to limit lateral movement for attackers within your organization's infrastructure. Restrict access to critical systems and data.

Monitoring and Detection: Deploy IDS and intrusion prevention systems to detect and block malicious activities, such as unusual network traffic patterns or known attack signatures.

Potential MITRE ATT&CK TTPs

TA0011 Command and Control	TA0005 Defense Evasion	TA0003 Persistence	TA0002 Execution
TA0042 Resource Development	TA0010 Exfiltration	TA0011 Command and Control	TA0043 Reconnaissance
TA0040 Impact	T1090 Proxy	T1140 Deobfuscate/Decode Files or Information	T1496 Resource Hijacking
T1027 Obfuscated Files or Information	T1591 Gather Victim Org Information	T1071.001 Web Protocols	T1071 Application Layer Protocol
T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1584.005 Botnet	T1584 Compromise Infrastructure
T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1588.005 Exploits			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad[.]onion/cmd1, http://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad[.]onion/kill, hxxp://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad[.]onion/mine, hxxp://ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad[.]onion/ping
Domains	p2pool[.]it, ru6r4inkaf4thlgflg4iqs5mhqwqubols5qagspvya4whp3dgbvmyhad[.]onion
IPv4	**92[.]204[.]243[.]155**
SHA256	1d489a41395be76a8101c2e1eba383253a291f4e84a9da389c6b58913786b8ac, d7843904e1c25055e14cae8b44b28f9dd4706c0ad8b03f55dfcded36ce8423a0, 4feb3dcfe57e3b112568ddd1897b68aeb134ef8addd27b660530442ea1e49cbb, f93e9bc9583058d82d2d3fe35117cbb9a553d54e7149846b2dc94446f0836201, 1d0c3e35324273ffeb434f929f834b59dcc6cdd24e9204abd32cc0abefd9f047, 0a8779a427aba59a66338d85e28f007c6109c23d6b0a6bd4b251bf0f543a029f, 153b0d0916bd3150c5d4ab3e14688140b34fdd34caac725533adef8f4ab621e2, 1c49d7da416474135cd35a9166f2de0f8775f21a27cd47d28be48a2ce580d58d, 21a9f094eb65256e0ea2adb5b43a85f5abfbfdf45f855daab3eb6749c6e69417, 371319cd17a1ab2d3fb2c79685c3814dc24d67ced3e2f7663806e8960ff9334c, 601a2ff4a7244ed41dda1c1fc71b10d3cfefa34e2ef8ba71598f41f73c031443, 9f740c9042a7c3c03181d315d47986674c50c2fca956915318d7ca9d2a086b7f, e71caf456b73dade7c65662ab5cf55e02963ee3f2bfb47e5cffc1b36c0844b4d

Patch Details

Upgrade to the versions of 5.1.2 or above for RocketMQ 5.x or 4.9.7 or above for RocketMQ 4.x

Link:
https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp

https://lists.apache.org/thread/m614czxtpvlztd7mfgcs2xcsg36rdbnc

References

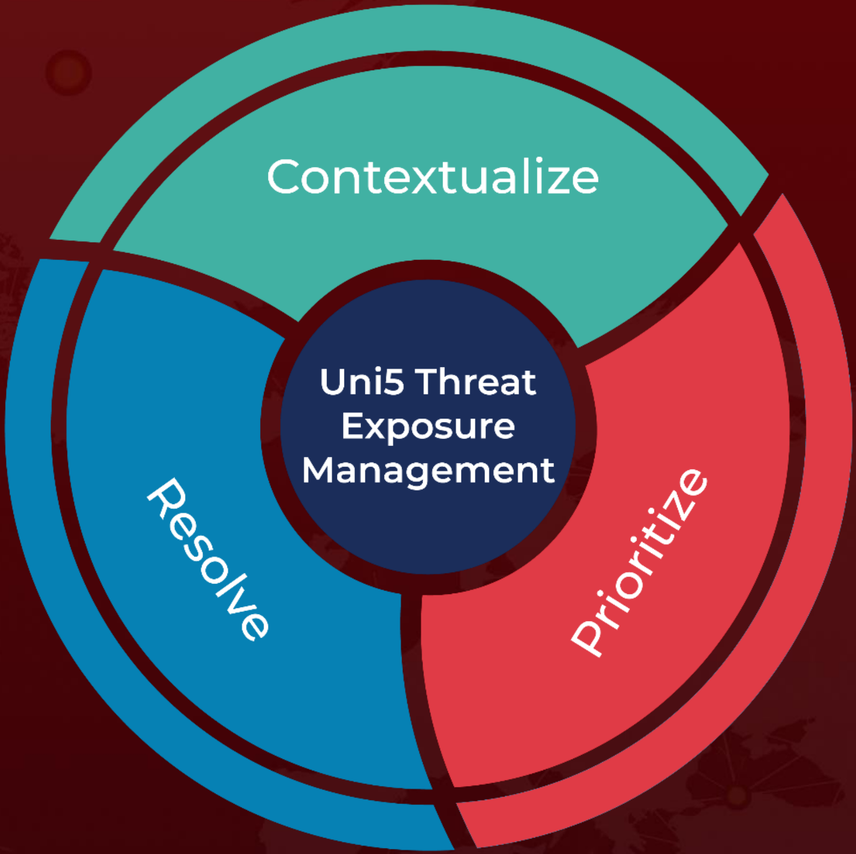
https://blogs.juniper.net/en-us/threat-research/dreambus-botnet-resurfaces-targets-rocketmq-vulnerability

https://blogs.juniper.net/en-us/threat-research/cve-2023-33246-apache-rocketmq-remote-code-execution-vulnerability

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 7, 2023 • 5:30 AM

More at www.hivepro.com